- 1 -

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

DAVID LEIBOWITZ, BENJAMIN LEIBOWITZ, JASON LEIBOWITZ, AARON LEIBOWITZ, and PINCHAS GOLDSHTEIN
 	
          Plaintiffs,
 	
v.
 	
IFINEX INC., BFXNA INC., BFXWW INC., TETHER HOLDINGS LIMITED, TETHER OPERATIONS LIMITED, TETHER LIMITED, TETHER INTERNATIONAL LIMITED, DIGFINEX INC., PHILIP G. POTTER, GIANCARLO DEVASINI, LUDOVICUS JAN VAN DER VELDE, REGINALD FOWLER, CRYPTO CAPITAL CORP., and GLOBAL TRADE SOLUTIONS AG,
 	
          Defendants.
	Case No. 1:19-cv-09236-KPF
	
	Honorable Katherine Polk Failla

<u>Affidavit of Michael Perklin</u>

- 1 -

I, Michael Perklin, declare under penalty of perjury, as follows:

1.   I am over the age of eighteen (18), I am not a party to this action, and I currently reside in Denver, Colorado. I have been retained as an expert in this matter.

2.   I base the facts and opinions in this declaration on my personal knowledge, education, experience, and documents provided to me by counsel. If called as a witness, I could and would testify to the truth of these facts and opinions under oath.

3.   I believe that my education and experience fully qualify me to make the statements contained in this declaration.

4.   I earned my diploma in computer sciences in 2004, my bachelor's degree in applied information sciences (information security) in 2009, both from Sheridan College. I then went on to earn my masters degree in information assurance, information security in 2011 from Davenport University. I hold the Certified Bitcoin Professional (CBP) designation, as well as Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).

5.   I was a digital forensic investigator for 8 years, spending 4 of them investigating blockchain systems exclusively. Since then, I have acted as the Chief Information Security Officer (CISO) of ShapeShift AG for 3 years, which operates a leading blockchain platform for the public. My numerous investigations have lead me to serve as an expert witness in two separate countries, and the evidence and recommendations delivered by my investigations have assisted dozens of companies around the world in securing their blockchain systems, and have placed attackers of those systems behind bars. I act as an advisor to a company that builds blockchain forensic analysis systems, I have taught courses on blockchain forensics and investigations, and I am the principal author of the

CryptoCurrency Security Standard (CCSS) which is regularly referenced by blockchain companies and governments around the world as they write new laws and regulations that affect blockchain technologies.

6.   I set forth additional facts about my background and qualifications in my curriculum vitae, attached as Exhibit A.

7.   Blockchain data is readily available to the public and can be retrieved with minimal effort from many sources by anyone sufficiently familiar with blockchain systems.

8.   Professor John Griffin's report, "Is Bitcoin Really Un-Tethered?," utilizes such publicly available blockchain data from the Bitcoin and Tether blockchains.

9.   Data referenced in the *Young* Complaint is similarly retrievable by querying the Bitcoin, Ethereum, EOS, and Tron blockchains.

Dated: January 27, 2020

MICHAEL PERKLIN

Michael Perklin, *CBP, CISA, CISSP, EnCE, ACE*

Contact Information

Cell: +1 (416) 992-6953
Email: michael@perklin.ca
Twitter: @mperklin
LinkedIn: https://ca.linkedin.com/in/perklin

Qualifications
Michael holds the following degrees and certifications:

Master of Science in Information Assurance (MSIA), University of Davenport, Davenport, Michigan

Bachelor of Applied Information Sciences (Information Systems Security) (BaISc), Sheridan Institute, Oakville, Ontario

Computer Science Technology diploma (CST), Sheridan Institute, Oakville, Ontario

Reid Technique of Interview and Interrogation - Advanced

Certified Bitcoin Professional (CBP)
#1a83e6

Certified Information Systems Security Professional (CISSP)
#443796

Certified Information Systems Auditor (CISA)
#14115468

Encase Certified Examiner (EnCE)
#15-0911-4347

AccessData Certified Examiner (ACE)
#UR-fc1p7132e98qw32-1229715

Affiliations
Michael is proud to be affiliated with the following organizations:

- CryptoCurrency Certification Consortium (C4), President (2014-Present)

- Bitcoin Alliance of Canada (BAC), Director (2013-2016); Lifetime Member (2013-Present)

- Bitcoin Foundation (BF), Lifetime Member (2013-Present); Director (2015-2019)

- High Technology Crime Investigations Association (HTCIA) (2008-2016)

- Association of Certified Forensic Investigators (ACFI) (2009-2016)

- Program Advisory Council (PAC) for the Bachelor of Information Sciences program at Sheridan Institute (2009-2015)

- Toronto Area Security Klatch (TASK) (2010-2016)

Statement of Qualifications   Michael **Perklin**

Relevant Experience

Michael founded Canada's first blockchain security consulting company, Bitcoinsultants, in 2012 after working in the Information-Security field for nearly a decade. Since then, he has earned an industry-wide reputation for best-in-class blockchain security consultations and cryptocurrency security audits.

Relevant experience includes:

- Conducted investigations into multiple high-profile breaches of cryptocurrency systems including Bitfinex (2016) and ShapeShift (2016)

- Trained law enforcement personnel in the traceability of cryptocurrencies

- Lead a digital-forensic investigation across multiple countries that culminated in the arrest and conviction of a cryptocurrency thief in Dubai, UAE

- Primary author and editor of the CryptoCurrency Security Standard - a collection of security controls gleaned from the study of dozens of information systems (both breached and secured)

- Design, implementation, and deployment of a high-security bitcoin vault system for the Ethereum crowdsale which raised and securely stored over 30,000 BTC

- Software Architecture and Engineering consultation with dozens of clients designing blockchain-based information systems to ensure security and assurance of funds

- Security consultation for Initial Coin Offerings (ICOs) that launched new cryptocurrencies including Ethereum, Factom, BreakoutCoin, Zcash

- Performed source code audits of web applications to identify security vulnerabilities and misuse of cryptographic libraries

- Advised the Canadian Senate Banking Committee on bitcoin technology and cryptocurrency investigations

- 1 year as Head of Security and Investigations at Ledger Labs Inc., a leading blockchain consultancy firm

- 3 years as bitcoin, cryptocurrency and blockchain security consultant at Bitcoinsultants Inc., the world's first blockchain security consultancy firm

- 2 years as lead digital investigator for Rogers Communications, one of the world's largest telecommunications companies where he lead hundreds of digital investigations.

- 3 years as digital-forensic and security consultant for Froese Forensic Partners, a boutique forensic firm based out of Toronto, ON where he performed forensic examinations on thousands of digital devices.

- Professor of Digital Forensics, Information Systems Auditing, and Computer Security courses in a Bachelor's degree security program

Cryptocurrency Projects

Michael is involved in a variety of cryptocurrency related projects:

- CryptoCurrency Security Standard - The world's first formal standard for cryptocurrencies. Michael worked with industry-recognized security experts to collect and analyze information about the world's most successful and least successful cryptocurrency systems. This data was used to author the world's first standard that applies to cryptocurrencies, allowing anyone to measure a company's security practices against a common scale. Michael currently serves as the chairman of the CCSS Steering Committee.

- Certified Bitcoin Professional - The world's first personnel certification for cryptocurrencies. Michael worked with Bitcoin experts around the world to build a database of peer-reviewed exam questions for the world's first cryptocurrency certification.

- Blockchain Training Conference - The world's first blockchain conference targeted at people *outside* the blockchain industry. Michael was lead organizer of this Toronto-based conference that trained lawyers, accountants, developers, auditors, traders, and anti-money-laundering specialists in how blockchains work and how they will impact the world in the very near future.

- Coindroids - The world's first role-playing game played with a blockchain. Michael provides technical and security consultation to this fascinating new video game concept that is played with cryptocurrency wallets.

- Bitcoin Intelligence Group - Advisor. Michael assists BIG's board of directors as an advisor where he provides insight into blockchain investigations. Michael's experience and advice has lead to the development of new features in their QLUE product which assist blockchain investigators in their investigations.

- SALT Lending - CyberSecurity Advisor. Michael assists SALT Lending's board of directors as a security advisor, providing advice and strategies to help build a secure lending system for their clients.

- Electrum - An open-source bitcoin wallet. Michael has contributed enhancements to Electrum which added a high-security feature allowing offline computers and online computers to communicate solely with QR-codes, removing the opportunity for malware to infect offline systems.

Publications

Michael has contributed the following papers to the information security community:

- "You Are What You Play": Breaching privacy and identifying users in online gaming, Transactions of the 12th Annual PST (Privacy, Security, Trust) IEEE Conference, Ryerson, Toronto, Canada, July 23-24, 2014

- Dealing with CryptoWall and Ransomware Decentral Blog, August, 2014

- Bitcoin Handbook for Non-Profits Bitcoin Foundation, October, 2014

Statement of Qualifications   Michael **Perklin**

Speaking Engagements

Michael has been invited to speak at the following conferences and venues internationally:

- *Thefts, Breaches, and Attacks - When Things Go Wrong*
  Blockchain:Money, London. November, 2016

- *Technology and Innovation Panel: Blockchain*
  ACAMS Canada, Toronto. Ontario, 2016

- *Blockchain Investigations*
  Blockchains, Cryptocurrencies, and AML, Toronto. August, 2016

- *The Future of Blockchains*
  Blockchain World Congress, New York. September, 2016

- *Blockchain Investigations*
  Blockchain Training Conference, Toronto. June, 2016

- *CCSS In Depth*
  Blockchain Training Conference, Toronto. June, 2016

- *Applying CCSS*
  Blockchain Training Conference, Toronto. June, 2016

- *Blockchains and Accounting*
  YDCPAA, Toronto. January, 2016

- *Bitcoin and Why it Matters*
  Ivey Alumni Network, Toronto. June, 2015

- *Securing Bitcoin and reaching CCSS Level III*
  Texas Bitcoin Conference, Texas. April, 2015

- *Bitcoin and Financial Technology*
  FISD Conference, New York. December, 2014

- *Bitcoin Security*
  Latin American Bitcoin Conference, Rio De Janeiro Brazil. December, 2014

- *The Bitcoin Startup Ecosystem*
  Inside Bitcoins, Las Vegas NV. October, 2014

- *Witness on Bitcoin and Cryptocurrencies Senate Committee on Banking, Trade, and Commerce*, Ottawa ON. October, 2014

- *ACL Steganography*
  Lockdown, Madison WI. June, 2014

- *Bitcoin and Financial Technology*
  FISD Conference, Toronto. May, 2014

- *High Security Bitcoin*
  Bitcoin Expo 2014, Toronto. April, 2014

- *Cyber-Security Panel*
  Bitcoin Expo 2014, Toronto. April, 2014

- *Bitcoin - Myths and Realities.*
  Ontario Securities Commission, Toronto. February, 2014

- *The State of Cyber Security*
  FISD Conference, Toronto. November, 2013

- *Forensic Fails*
  DEF CON 21, Las Vegas. August, 2013

- *ACL Steganography*
  DEF CON 21, Las Vegas. August, 2013

- *Bitcoin 101 for Cyber Investigators*
  HTCIA Ontario Chapter, Toronto. April, 2013

- *Bitcoin for Lawyers - Up to Speed in 60m*
  [Redacted], Toronto. May, 2012

- *Anti-Forensics and Countermeasures*
  SECTOR, Toronto. October, 2012

- *Anti-Forensics and Anti-Anti-Forensics*
  DEF CON 20, Las Vegas. July, 2012

- *Defence In Depth - Don't Stop in the Middle*
  pgWest Conference, San Jose. September, 2011

- *Dealing with Computer Crime - Demystifying the Myth*
  ACFI Fraud Conference, Toronto. July 2009